Wisconsin Enterprise Architecture Team's Comments to the proposed ID/Password Management Standard from the Information Security and Privacy Domain

The distributed nature of computing has made it extremely difficult for enterprises to gain a level of comfort in the authentication and authorization of a diverse set of users. Large enterprises, such as the State of Wisconsin, must deal with a diverse set of operating systems, databases and applications. The number of components in the environment, and the variety among them, is increasing. New application systems are being developed — as well as applications for new classes of users — with unprecedented scale requirements. Thus the State faces the complicated task of managing how users are identified and authenticated, and how their privileges are defined and managed.

However, security is not and cannot be absolute. Therefore the risks assumed by a proposed policy or standard need to balance properly against the business impact. And determining the balance point between the potential for a security breach and the implementation of new security measures upon business users tends to be controversial.

Almost every government entity with a user identification and password policy has used a risk and assurance level determination scheme that stratifies risk levels and coincident assurance requirements into three or more tiers, such as minimum, low, and high. WEAT recommends that the Information Security and Privacy domain reevaluate the proposed ID/Password Management Standard from this perspective and determine where and when which types of security authorization are necessary. This approach will hopefully help to balance the risks associate with a security breach and the implementation of new security measures upon business users.